AMENDMENT TO THE CLAIMS

1. (Currently Amended) A system comprising:

a first non-volatile data storage device, configured as ~~one or more~~a plurality of storage regions~~,~~ to store ~~one or more bytes of~~ CMOS memory data, wherein the device lacks hardware security such that some of the CMOS memory data storage regions are modifiable by an application program on the system, each of the regions being protected by at least two software schemes including a set of one or more region level rules and another scheme selected from the group consisting of (1) mask bits, (2) checksum, (3) cyclic redundancy check, CRC, and (4) encryption;

another, second non-volatile data storage device to store a mirror image of the CMOS memory data in a locked location ~~that cannot be modified without system authorization~~;

a program store to store ~~one or more~~ processor-readable instructions ~~to~~ that implement each of the software schemes to ascertain the validity of the CMOS memory data stored in the first non-volatile storage device on a region by region basis and, when data stored in any one of the storage regions is found to be invalid ~~to~~, replace the CMOS memory data in said one of the storage regions of the first non-volatile storage device with the stored mirror image of the data; and

a processing unit coupled to the first and second non-volatile data storage devices and program store, to read and process the one or more instructions in the program store.

2. (Previously Presented) The system of claim 1 wherein the processing unit is to process the instructions in the program store as part of a start-up procedure.

3. (Previously Presented) The system of claim 1 wherein the program store is inside said second non-volatile data storage device.

Claims 4-5 (Canceled).

6. (Currently Amended) The system of claim 4 wherein ~~system authorization includes~~

~~employing a system interface to perform modifications to the data stored in said second non-volatile data~~the processing unit is to compare mask bits, cyclic redundancy

check, and/or checksum of the content in each of the plurality of storage regions to previously stored corresponding values, in order to ascertain the validity of the CMOS memory data stored in the first non-volatile storage device.

7. (Currently Amended) The system of claim 1 wherein ~~ascertaining the validity of the CMOS memory data stored in the first non-volatile storage device includes~~

~~determining if current data in the first non-volatile storage device is different than the stored image of the data~~the region level rules define which bit of a particular byte in a given storage region holds a mask bit.

8. (Currently Amended) The system of claim 1 wherein ~~ascertaining the validity of the CMOS memory data stored in the first non-volatile storage device includes~~

~~determining if an integrity metric corresponding to current data in the first non-volatile storage device is different than the same integrity metric corresponding to the stored image of the data~~the region level rules define which byte of a given storage region holds a mask bit, which byte holds a checksum, and which byte holds a CRC value.

9. (Previously Presented) The system of claim 1 further comprising:

generating a copy of current data in the first non-volatile storage device when an authorized application modifies the current data; and

storing the copy as a valid image of the current data.

10. (Currently Amended) A method comprising:

reading CMOS memory content stored in a plurality of storage regions of a first non-volatile storage device of a system, wherein the first device lacks hardware security such that the CMOS memory content is modifiable by an application program in the system, each of the regions being protected by at least two software schemes which include a set of region level rules and another scheme selected from the group consisting of (1) mask bits, (2) checksum, (3) CRC, and (4) encryption;

reading from a valid image of the CMOS memory content, that is stored in a further, second non-volatile storage device;

determining when the CMOS memory content in the first device has been modified without authorization by comparing a previously stored checksum,

corresponding to the valid image of the CMOS memory content within only a selected one of the plurality of storage regions, and a checksum corresponding to the CMOS memory content within said selected one of the storage regions, and by comparing a previously stored cyclic redundancy check value, corresponding to the valid image of the CMOS memory content within only a selected further one of the storage regions, and a cyclic redundancy check value corresponding to the CMOS memory content within said selected further one of the storage regions; and

replacing the CMOS memory content with said stored valid image when the CMOS memory content is determined to have been modified without authorization.

11. (Currently Amended) The method of claim 10 wherein the determining comprises:

comparing the valid image of the CMOS memory content within a still further one of the storage regions to the CMOS memory content within said still further one of the storage regions to determine when the CMOS memory content has been modified.

Claims 12-13 (Canceled).

14. (Currently Amended) The method of claim 10 wherein determining when the CMOS memory_content has been modified without authorization further includes

comparing a previously stored bit mask, corresponding to the valid image of the CMOS memory content within only the selected one or the selected further one, of the storage regions, and a bit mask corresponding to the CMOS memory content within said selected one or said selected further one of the storage regions.

15. (Previously Presented) The method of claim 10 further comprising:

storing a valid image of the CMOS memory content for later use.

16. (Previously Presented) The method of claim 10 wherein reading the CMOS memory content from the first non-volatile storage device is part of a start-up procedure of the system.

17. (Currently Amended) A method comprising:

arranging a first non-volatile storage device of a computer system into ~~one or more~~a plurality of storage regions to store CMOS data, wherein the device lacks

hardware security such that some of the ~~CMOS~~ storage regions are modifiable by an application program in the system, each of the regions being protected by at least two software schemes including a set of region level rules and another scheme selected from the group consisting of (1) mask bits, (2) checksum, (3) CRC, and (4) encryption;

generating ~~an~~ a first integrity metric corresponding to mask bits of valid CMOS content stored in a first region of the first non-volatile storage device; ~~and~~

generating a second integrity metric corresponding to encryption of valid CMOS content stored in said first region of the first non-volatile storage device;

storing the first and second integrity ~~metric~~ metrics in another, second non-volatile storage device of the computer system to later determine when the content in the first region has been modified without authorization.

18. (Previously Presented) The method of claim 17 further comprising:

comparing a previously stored integrity metric, corresponding to an earlier version of the content stored in the first region, to a newly calculated integrity metric corresponding to the current content stored in the first region to determine when an unauthorized modification has occurred.

19. (Currently Amended) The method of claim ~~17~~ 18 further comprising:

replacing the content of the first region with an earlier version of the content therein when it is determined that there was an unauthorized modification.

Claims 20-30 (Canceled).